EXPRESS MAIL NO. EL594196325US

METHOD FOR MANAGING SECURITY OF NETWORK SYSTEM

Patent Number: JP11025048
Publication date: 1999-01-29
Inventor(s): SAITO YOKO; SHIMIZU MICHIHIRO; IKEUCHI MANABU
Applicant(s):: HITACHI LTD
Requested Patent: ☐ JP11025048
Application Number: JP19970173532 19970630
Priority Number(s):
IPC Classification: G06F15/00 ; G06F13/00 ; H04L9/32
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To attain single sign-on while holding high level security in a closed network by down-loading a certificate corresponding to a transaction from a certification server according to the input of a synthetic certificate, and executing the certification of a communicated party and the encipherment of communication based on the information of the certificate.
SOLUTION: At the time of inputting a synthetic certificate from a client 8 or client 20 connected with another enterprise network system 9, and for example, logging-in a DB server 5, a synthetic certification server 2 confirms the synthetic certificate, and transmits the certificate information of the person concerned to the client 8 or the client 20 and the DB server 5 when access authority is present, and a processing between the client 8 or 20 and the DB server 5 is started. When the client logs in a task server 6, the certificate information of the person concerned is transmitted from the synthetic certification server 2 to the client 8 or the client 20 and the task server 6 so that single sign-on can be realized.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－25048

(43)公開日　平成11年(1999)１月29日

(51)Int.Cl.[6]		識別記号	F I		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｂ
	13/00	３５７		13/00	３５７Ｚ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ
					６７５Ｄ

審査請求　未請求　請求項の数５　ＯＬ　（全　８　頁）

(21)出願番号　特願平9－173532

(22)出願日　平成９年(1997)６月30日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　齋藤　洋子
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　清水　道浩
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

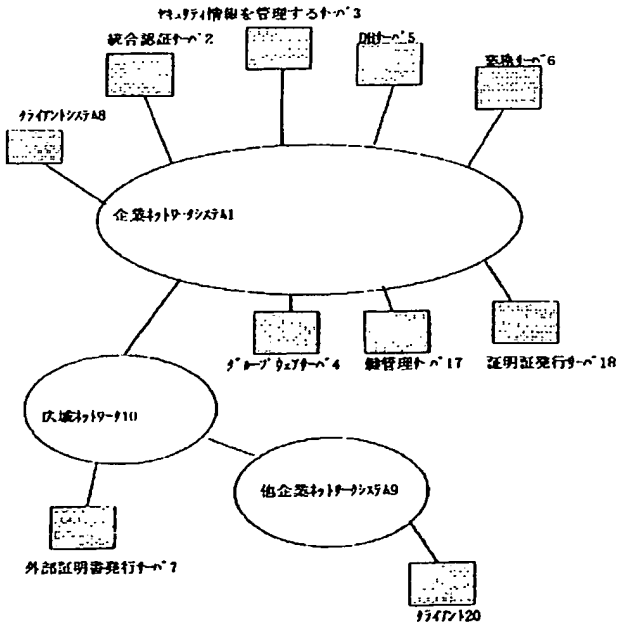
(72)発明者　池内　学
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　ネットワークシステムのセキュリティ管理方法

(57)【要約】
【課題】インターネットのような広域ネットワークシステムと企業内ネットワークシステムとを統合したネットワークにおける通信時の高セキュリティを実現する。
【解決手段】クライアント及びサーバが通信を行うネットワークシステムにおいて、クライアントから統合認証サーバへ統合証明書の情報を送信して認証要求を行い、ユーザのアプリケーションのアクセス権限または通信相手への通信権限が正当であれば通信の当事者に対してクライアントあるいは通信先の証明書を送信し、クライアントは通信先への通信メッセージを証明書の情報と対になるクライアント固有の鍵情報を用いて暗号化し、通信先では証明書の情報によりクライアントを確認し、通信メッセージを復号化する。通信先では、クライアントへの通信メッセージを証明書の情報と対になる通信先固有の鍵情報を用いて暗号化し、クライアントは証明書の情報により通信先を確認し、前記通信メッセージを復号化する。

図１



1

【特許請求の範囲】

【請求項1】ネットワークを介してクライアント及びサーバが通信を実行するネットワークシステムにおいて、クライアントから統合認証サーバへ統合証明書の情報を送信して認証要求を行い、統合認証サーバによって統合証明書の確認とクライアントのユーザ認証処理を行い、クライアントから業務サーバのアプリケーションあるいは通信相手への通信要求について、統合認証サーバによってユーザの該アプリケーションへのアクセス権限あるいは通信相手への通信権限のチェックを行い、前記チェックが正当であれば通信の当事者に対してクライアント、業務サーバあるいは通信相手の証明書を送信し、クライアントは業務サーバあるいは通信相手への通信メッセージを前記証明書の情報と対になるクライアント固有の鍵情報を用いて暗号化し、業務サーバあるいは通信相手では前記証明書の情報によりクライアントを確認し、前記通信メッセージを復号化し、業務サーバあるいは通信相手はクライアントへの通信メッセージを前記証明書の情報と対になる業務サーバあるいは通信相手固有の鍵情報を用いて暗号化し、クライアントでは前記証明書の情報により業務サーバあるいは通信相手を確認し、前記通信メッセージを復号化することを特徴とするネットワークシステムのセキュリティ管理方法。

【請求項2】統合認証サーバによって統合証明書の確認を行う代わりに、クライアント、業務サーバあるいは通信相手が通信の当事者の証明書を事前に管理し、統合認証サーバに証明書取り消しリストを要求することにより、クライアントが通信要求する時に業務サーバあるいは通信相手の証明書が有効であることを前記証明書取り消しリストの情報によりチェックし、前記チェックが正当であればクライアントは業務サーバあるいは通信相手への通信メッセージを前記証明書の情報と対になるクライアント固有の鍵情報を用いて暗号化し、業務サーバあるいは通信相手では前記証明書の情報によりクライアントを確認し、前記通信メッセージを復号化し、業務サーバあるいは通信相手ではクライアントの証明書が有効であることを前記証明書取り消しリストの情報によりチェックし、前記チェックが正当であれば業務サーバあるいは通信相手はクライアントへの通信メッセージを前記証明書の情報と対になる業務サーバあるいは通信相手固有の鍵情報を用いて暗号化し、クライアントでは前記証明書の情報により業務サーバあるいは通信相手を確認し、前記通信メッセージを復号化することを特徴とするネットワークシステムのセキュリティ管理方法。

【請求項3】請求項2において、クライアント、業務サーバあるいは通信相手に対して、統合認証サーバが証明書取り消しリストを自動的に配送することを特徴としたネットワークシステムのセキュリティ管理方法。

【請求項4】ネットワークを介してクライアント、業務サーバあるいは通信相手および統合認証サーバが相互に

2

通信可能なネットワークシステムの当該統合認証サーバによって読み取り可能な記憶媒体上に記憶されたコンピュータプログラムであって、該プログラムは以下のステップを含む：

（a）クライアントから送信された統合証明書の情報を受信し、（b）該統合証明書が正当であることを確認し、（c）該統合証明書のユーザが該業務サーバあるいは通信相手にアクセスする権限があるか否かをチェックし、（d）（b）および（c）のチェック結果が妥当であれば、通信の当事者に対して証明書を送信する。

【請求項5】ネットワークを介してクライアント、業務サーバあるいは通信相手および統合認証サーバが相互に通信可能なネットワークシステムの当該統合認証サーバによって読み取り可能な記憶媒体上に記憶されたコンピュータプログラムであって、該プログラムは以下のステップを含む：

（a）通信要求のあったクライアントに対して証明書取り消しリストを送信し、（b）クライアントの認証が必要な業務サーバあるいは通信相手に対して証明書取り消しリストを送信する。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークを介して通信を行うクライアント、サーバー間の通信方法に関し、特に広域ネットワークシステムにおいて証明書を利用してユーザ認証及びアクセス制御を行う認証サーバを備えたネットワークシステムのセキュリティ管理方法に関する。

【0002】

【従来の技術】インターネットの普及に伴いセキュリティをめぐる市場動向はめざましく変化してきた。特に、インターネットとイントラネットを統合する認証サーバは重要であり、広域ネットワークシステムでユーザを一元管理しさらに集中的にアクセス制御を行う機能が求められている。

【0003】一方、昨今の電子商取引や通信では、公開鍵ベースの証明書を用いた認証処理と通信の暗号処理が主流になってきている。

【0004】

【発明が解決しようとする課題】発明者らは既に出願した特願平9-76954号により、インターネットのような広域ネットワークシステムと企業内ネットワークシステムとを統合するためにユーザ認証機能およびネットワークシステム内の資源へのアクセス制御機能に関して出願しているが、より現実的に実用化を考慮した際、証明書自体の管理と運用面での考慮が必要と考えた。

【0005】本発明では、統合証明書を元にユーザの認証情報を参照する事によるシングルサインオンの実現方式、および統合証明書を元に業務ごとの証明書や証明書取り消しリストを通信の当事者にダウンロードすること

によるユーザ認証および通信暗号化処理のためのセキュリティ管理を実現するものである。

【0006】

【課題を解決するための手段】前記統合証明書の入力により取引に応じた証明書を認証サーバからダウンロードし、前記証明書の情報により通信相手の認証と通信の暗号化を実現する。

【0007】本発明は、ネットワークを介してクライアント、業務サーバあるいは通信相手および統合認証サーバが相互に通信可能なネットワークシステムのセキュリティ管理方法であって、クライアントから統合認証サーバに対して統合証明書の情報を送信してクライアントのユーザの認証要求を行い、クライアントから業務サーバのアプリケーションあるいは通信相手への通信要求に対して、統合認証サーバでアクセス権限をチェックし、正当であれば通信の当事者に証明書を送付し、クライアントは業務サーバあるいは通信相手への通信メッセージを前記証明書の情報と対になるクライアント固有の鍵情報を用いて暗号化し、業務サーバあるいは通信相手側では前記証明書の情報によりクライアントを確認し、前記通信メッセージを復号化し、業務サーバあるいは通信相手はクライアントへの通信メッセージを前記証明書の情報と対になる業務サーバあるいは通信相手固有の鍵情報を用いて暗号化し、クライアントでは前記証明書の情報により業務サーバあるいは通信相手を確認し、前記通信メッセージを復号化する統合証明書によるセキュリティ管理方法を特徴とする。

【0008】なお、統合認証サーバにより通信の当事者の証明書をダウンロードする代わりに、通信の当事者で前記証明書を管理し、統合認証サーバに証明書取り消しリストを要求することにより、クライアントが通信要求する時に業務サーバあるいは通信相手の証明書が有効であることを前記証明書取り消しリストの情報によりチェックし、前記チェックが正当であればクライアントは業務サーバあるいは通信相手への通信メッセージを前記証明書の情報と対になるクライアント固有の鍵情報を用いて暗号化し、業務サーバあるいは通信相手では前記証明書の情報によりクライアントを確認し、前記通信メッセージを復号化し、業務サーバあるいは通信相手ではクライアントの証明書が有効であることを前記証明書取り消しリストの情報によりチェックし、前記チェックが正当であれば業務サーバあるいは通信相手はクライアントへの通信メッセージを前記証明書の情報と対になる業務サーバあるいは通信相手固有の鍵情報を用いて暗号化し、クライアントでは前記証明書の情報により業務サーバあるいは通信相手を確認し、前記通信メッセージを復号化するようにしてもよい。

【0009】

【発明の実施の形態】以下本発明の一実施形態について図面を用いて説明する。

【0010】図1は、本実施形態のネットワークシステムの構成図である。

【0011】インターネットの様な広域ネットワーク10に、企業ネットワークシステム1と他企業ネットワークシステム9が接続されている。

【0012】企業ネットワークシステム1は、クライアント8の他に、統合認証サーバ2、セキュリティ情報を管理するサーバ3、データベース（DB）サーバ5、業務サーバ6、グループウェアサーバ4、鍵管理サーバ17、証明書発行サーバ18等のサーバが接続されている。

【0013】DBサーバ5および業務サーバ6は、クライアント8からアクセスされ、業務処理のために利用されるサーバである。

【0014】グループウェアサーバ4は、クライアント8へ最初の業務メニュー画面を送ったり、クライアント8へ電子メールを送ったり、ユーザのスケジュールを管理したりするサーバである。

【0015】他企業ネットワークシステム9には、クライアント20が接続しており、クライアント8のユーザとクライアント20のユーザは、電子取引等の特定の業務を証明書を用いて行う。

【0016】サーバ3は、DBサーバ5および業務サーバ6または他企業ネットワークシステム9へのアクセスを制御する情報と業務に応じた証明書の情報を含むユーザの認証情報とからなるセキュリティ情報を一元的に管理するサーバである。

【0017】統合認証サーバ2は、クライアント8から送られる統合証明書を確認し、サーバ3からセキュリティ情報を取得してユーザのDBサーバ5および業務サーバ6または他企業ネットワークシステム9へのアクセス権限をチェックし、チェック結果が正当であれば通信の当事者に対して業務に応じた証明書や証明書の取り消しリストを送信するサーバである。

【0018】鍵管理サーバ17は、企業ネットワークシステム1内での暗号化通信で使用する通信の当事者の鍵（秘密鍵と公開鍵の対）を生成するサーバである。

【0019】広域ネットワーク10には外部証明書発行サーバ7が接続される。外部証明書発行サーバ7は、所定の手順に従って外部証明書を発行するサーバである。証明書発行サーバ18は、統合認証サーバ2からの要求によって統合証明書を発行するサーバである。なおいわゆるディレクトリサーバと呼ばれるサーバがサーバ3の情報を有していてもよい。また、クライアント8および各種サーバは、パソコン、ワークステーション等を含む情報処理装置である。

【0020】さらにクライアント8および各種サーバによって各々読み取り可能な記憶媒体上に実体化されたコンピュータプログラムを実行して以下に詳述するクライアント8および各種サーバの処理を行うことができる。

5

【0021】クライアント8または他企業ネットワークシステム9に接続されるクライアント20から統合証明書の情報を入力して例えばDBサーバ5にログインすると、統合認証サーバ2が統合証明書の確認を行い、統合認証サーバ2がサーバ3からセキュリティ情報を取得してDBサーバ5へのアクセス権限をチェックする。アクセス権限があれば、クライアント8またはクライアント20、およびDBサーバ5に対して通信の当事者の証明書情報を送り、クライアント8または20とDBサーバ5間の処理が始まる。

【0022】クライアントはDBサーバ5への通信メッセージを前記証明書の情報と対になるクライアント固有の鍵情報（以降秘密鍵と呼ぶ）を用いて暗号化し、DBサーバ5では前記証明書から取り出したクライアントの公開鍵によりクライアントを確認し、前記通信メッセージを復号化する。

【0023】また、DBサーバ5でも、クライアントへの通信メッセージを前記証明書の情報と対になるDBサーバ5の秘密鍵で暗号化し、クライアントでは前記証明書から取り出したDBサーバ5の公開鍵により相手を確認し、前記通信メッセージを復号化することが可能である。

【0024】このように、統合証明書の情報から取引に必要な証明書情報が取り出され、しかも統合認証サーバ2が保持する最新の証明書取り消しリストによりこれらの証明書の有効性が確認された後、通信の当事者に渡されるため、通信の当事者は証明書を管理しなくて済む。

【0025】また、クライアントが次に業務サーバ6にログインする時、統合認証サーバ2からクライアント8またはクライアント20、および業務サーバ6に対して通信の当事者の証明書情報が送られるので、シングルサインオンが実現される。

【0026】図2は、セキュリティ情報を管理するサーバ3がセキュリティ情報を一元管理する方式を説明する図である。

【0027】サーバ3を導入する前に各サーバごとに管理していたユーザおよび資源（文書、データベース、端末装置、アプリケーションプログラム等）に関するセキュリティ情報をLDAP情報変換ツールによりLDAP形式に変換し、サーバ3へ送ってサーバ3で一元管理する。ここに、LDAP(Lightweight Data Access Protocol)とは、IETF標準のディレクトリアクセスプロトコルである。

【0028】図3は、LDAP形式の情報の例として、文書の定義と業務サーバボアクセス制御情報および証明書情報の形式を示す図である。

【0029】文書の定義は、文書識別情報と文書のアクセス制御情報から構成される。文書識別情報は、文書の識別子、この文書を管理するサーバの識別子と組織名称、並びに文書の情報(文書のタイトル、文書の更新日付、文書管理者、文書検索のためのキーワード、主題、アブストラクト、作者名)から構成される。

6

【0030】一方、文書のアクセス制御情報は、アクセス制御情報、最終修正情報、セキュリティポリシー等を含む。アクセス制御情報は、文書内の特定ページのアクセス制御情報のように文書の一部についてアクセス制御をする情報である。

【0031】最終修正情報は、アクセス制御情報の更新日付である。セキュリティポリシーは、その文書にアクセスを許可するユーザのアクセスレベルを設定するものである。例えば、ポリシー番号が1から3までのユーザに当文書をアクセス許可するという運用が可能である。文書の定義は、業務サーバ6が管理する情報である。

【0032】図4は、統合認証サーバ2がサーバ3からユーザのセキュリティ情報を取得する手順を説明する図である。セキュリティ情報を取得する手順には、LDAPプロトコルが使用される。統合認証サーバ2は、まず、ldap_openによってサーバ3とLDAPコネクションを確立し、ldap_simple_bind_sによって統合認証サーバ3とサーバ3との間の相互認証を行った後、ldap_search_sによって統合認証サーバ2からユーザの統合証明書番号、ユーザID等を送信すると、サーバ3から統合認証サーバ2へそのユーザのセキュリティ情報を送信する。

【0033】図5は、クライアント8のユーザが企業ネットワークシステム1にログインしてからログオフするまでの処理の手順を示す図である。ここでは、ユーザが統合証明書を用いてログインする場合の手順について説明する。

【0034】クライアント8は、業務メニューをクライアント8の表示画面に表示する。ユーザが業務サーバ6を選択し、統合証明書の情報をICカード等の秘密情報格納媒体から入力すると、クライアント8は、統合証明書の情報をユーザの秘密鍵で暗号化して記憶装置に格納した後、業務要求とユーザの秘密鍵で暗号化された統合証明書の内容を統合認証サーバ2へ送信する。

【0035】統合認証サーバ2は、暗号化された統合証明書の情報をユーザの公開鍵で復号化した後、その統合証明書の確認を行う。

【0036】統合証明書のデータ構成は、X.509で規定されており、その内容は所有者氏名、発行元、発行元の署名、有効期限等の情報から成る。

【0037】発行元の署名は、発行者の秘密鍵で暗号化されているので、まず、この署名を発行元の公開鍵で復号化して原本と比較し、統合証明書が正当なものである事を確認する。次に有効期限など内容の確認を行う。統合証明書が不適当なものであれば(NG)、クライアント8へログイン不許可のメッセージを送信する。統合証明書が適切なものであれば(OK)、サーバ3へ問い合わせを行ってユーサのセキュリティ情報を取得する。その手順については上記した通りである。ユーザのセキュリティ情

報は、業務サーバ6のアクセス制御情報とユーザのアクセス制御情報、およびこの業務に必要な業務サーバ6とユーザの証明書から構成される。

【0038】統合認証サーバ2は、ユーザのアクセスレベルと業務サーバ6のアクセスレベルとを比較し、業務サーバ6のアクセスを許可できるならば、業務サーバ6およびユーザの業務に関する証明書を取り出し、最新の証明書取り消しリストを確認することにより、前記証明書の有効性を確認する。両者の証明書情報が有効であれば、当該ユーザのアクセスを許可する旨のアクセス履歴情報を記憶装置に記録し、業務サーバ6およびユーザに対して、両者の証明書情報を送信する。その際、証明書情報は受信者の公開鍵で暗号化して送るので、秘密鍵を持つ当事者しか証明書情報を復号化できない仕掛けになっている。

【0039】クライアント8からは業務サーバ6が保有する文書にアクセス要求をして業務処理を行う。その前に相互で認証処理を行うが、その処理手順については、図6で説明する。相互での認証処理が終了した後、クライアント8は業務サーバ6に対してデータを暗号化して送ることが可能になる。クライアント8は、業務サーバ6との間で認証処理の中でネゴシエーションしたセション鍵を用いて、メッセージを暗号化する。この暗号化処理は、クライアント8で行うためユーザは意識しなくて良い。前記暗号化されたメッセージは業務サーバ6の保持するセション鍵で復号化され、業務サーバ6だけが読むことができる。業務サーバ6からクライアント8にメッセージを送信する時も同様で、前記セション鍵を用いて暗号化/復号化される。通常のセション鍵は1回限り有効な使い捨ての鍵を用いるため、通信の機密性が高い。

【0040】また、本実施例では、認証処理の中でサーバ側がセション鍵を作成しているが、クライアント側で作成することも可能である。また、セション鍵の作成方法自体も、各取引のプロトコルシーケンスに従うものとする。

【0041】クライアント8は、業務処理の間、アクセスする文書についてアクセス履歴情報を記憶装置に記録する。

【0042】このようにして、業務サーバ6に係わる業務処理を終了した後、再び業務メニューをクライアント8の表示装置に表示する。ユーザが次にクライアント20との電子取引処理を選択したとすれば、クライアント8は記憶していた当該ユーザの統合証明書を取り出して業務要求と共に統合認証サーバ2へ送信する。従って、ユーザは再度統合証明書の情報を入力する必要がない。

【0043】以後上記と同様に統合認証サーバ2は、暗号化された統合証明書をユーザの公開鍵で復号化した後、統合証明書の確認を行い、統合証明書の確認結果問題なければ、当該ユーザの電子取引処理へのアクセスを許可/不許可する旨のアクセス履歴情報を記録する。

【0044】ユーザのアクセスを許可した時、クライアント8に、クライアント8および取引相手であるクライアント20の証明書の有効性を確認した後、証明書情報を通信の当事者に送信する。クライアント8は、証明書の情報を用いてクライアント20との間で電子取引処理を行い、取引処理の間、アクセス履歴情報を記録する。このようにして、処理を終了し、ユーザがログオフを入力すると、クライアント8は記録したアクセス履歴情報を統合認証サーバ2に送り、記憶装置上に保管していた統合証明書の情報を消去する。統合お認証サーバ2は、受信したアクセス履歴情報と統合認証サーバ2が記録したアクセス履歴情報を比較して、妥当なアクセスであるか否かをチェックする。

【0045】図6は、通信の当事者であるクライアント8、業務サーバ6間での相互認証処理の一例である。相互認証の方法は取引プロトコルに従うが、図6の例では、証明書とチャレンジの値を確認する方式で相互で認証している。

【0046】まず、クライアント8から業務サーバ6に対して、クライアント8のユーザの証明書をクライアントの電子署名を付与して送る。ここで電子署名とは、ユーザ名からハッシュ関数により作成した特殊なデータ列(例えばハッシュ値)をユーザの秘密鍵で暗号化した情報である。

【0047】業務サーバ6では、受信した署名を証明書に含まれるユーザの公開鍵で復号化することによりハッシュ値を取り出す。そして、ユーザ名から実際にハッシュ関数で値を作成し、受信したハッシュ値と一致するかどうかを確認する。さらに、受信した証明書が正当なものかどうかを確認し、全ての確認結果が正しければクライアント8のユーザを認証する。

【0048】次に、業務サーバ6は、セション鍵を作成し、それをユーザの公開鍵で暗号化した後、送信する。クライアント8は、受信した情報をユーザの秘密鍵で復号化し、セション鍵を取り出す。

【0049】すると、クライアント8側では、作成した乱数(チャレンジ)をセション鍵で暗号化して業務サーバ6に送信する。業務サーバ6側では、受信した情報をセション鍵で復号化することにより、チャレンジを取り出す。業務サーバ6は、チャレンジとサーバ名を業務サーバ6自身の秘密鍵で暗号化し、自分の証明書と共にクライアント8に送信する。クライアント8では、受信した情報を業務サーバ6の証明書に含まれる業務サーバ6の公開鍵で復号化し、チャレンジを取り出し、それが自分が業務サーバ6に送信した情報と一致するかどうかを確認する。さらに、業務サーバ名に付加された電子署名を検証し、全ての確認結果が正しければ業務サーバ6を認証する。

【0050】図7は、統合認証サーバ2による証明書の

有効性確認と送信処理を、通信の当事者で行う処理の一例である。

【００５１】図５との相違点は、通信の当事者が証明書の有効性の確認を行わなければならない点であり、証明書の確認処理の前に、統合認証サーバ２から最新の証明書取り消しリストをダウンロードして、通信相手の証明書が有効であるかどうかを確認する。証明書取り消しリストのダウンロードを自動的に行う運用も可能であり、例えば、システム立ち上げ時、最初の業務開始時、業務終了時等の指定をしておき、その契機でダウンロードを行うことができる。

【００５２】また、図７のシーケンス図では、クライアント８と業務サーバ６の双方に証明書取り消しリストを送付しているが、業務サーバ６に送付して、業務サーバ６からクライアント８に送付するような運用も可能である。電子取引の様々なプロトコルに従うものとする。

【００５３】以上、本発明を実施することにより、広域ネットワークシステム内のディレクトリサーバは、ネットワークシステムの資源に関する情報を一元管理しているので、統合認証サーバはディレクトリサーバからユーザの認証情報、アクセス制御情報、および証明書情報を取得できる。これにより、統合認証サーバは統合証明書によってユーザを認証し、ユーザのアクセスを制御できるので、企業ネットワークシステム内に統合証明書でアクセスさせるシングルサインオンを実現する。統合認証サーバは、統合証明書でユーザ認証、アクセス制御ができ、ユーザの業務要求に応じて有効な証明書を通信の当事者に送信できる。証明書を自分で管理する通信の当事者に対しても最新の証明書取り消しリストを送信するので、証明書を用いた相互認証、通信の暗号化処理を保証する。統合証明書を持つユーザの業務あるいは取引要求に対して、ユーザのアクセス要求が認められれば、通信の当事者に対して、業務あるいは取引の証明書を送信する。その際、統合認証サーバは、最新の証明書取り消しリストにより証明書の有効性を確認してから証明書を送信するので、通信の当事者は証明書は有効なものとして業務を開始できる。一方、通信の当事者が証明書を管理

して通信を行う場合には、通信の当事者が自分で証明書を管理し、最新の証明書取り消しリストにより証明書の有効性を確認してから業務を開始する必要がある。

【００５４】通信の当事者は、証明書の情報を用いて相互で認証とセション鍵の交換ができ、認証が終了した段階で、セション鍵を用いた通信の暗号化処理ができる。

【００５５】また、クライアントと統合認証サーバが連携することによって、ユーザのアクセス状況を監視することもできる。

【００５６】

【発明の効果】広域ネットワークと接続する企業ネットワークシステムの如く閉じたネットワークにおいて、高度なセキュリティを保持したまま、シングルサインオンを実現することができる。

【図面の簡単な説明】

【図１】実施形態のネットワークシステムの構成図である。

【図２】実施形態のサーバ３がセキュリティ情報を一元管理する方式について説明する図である。

【図３】LDAP形式の情報の例を示す図である。

【図４】実施形態の統合認証サーバ２がサーバ３からセキュリティ情報と証明書情報を取得する手順を示す図である。

【図５】実施形態の統合証明書を利用するシングルサインオンの処理手順を示す図である。

【図６】図５の処理手順の中の、通信の当事者間での相互認証とセション鍵の生成処理を説明する図である。

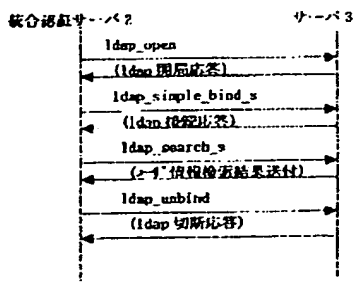
【図７】通信の当事者で証明書を管理し、最新の証明書取り消しリストにより証明書の有効性を確認する処理手順を説明する図である。

【符号の説明】

１…企業ネットワークシステム、２…統合認証サーバ、３…セキュリティ情報を管理するサーバ、６…業務サーバ、７…外部証明書発行サーバ、８…クライアント、１７…鍵管理サーバ、１８…統合証明書発行サーバ、２０…クライアント。

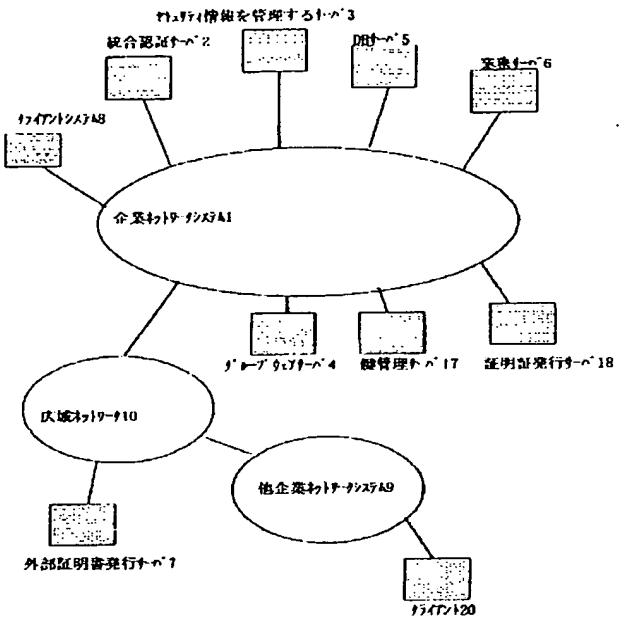
【図４】

図４



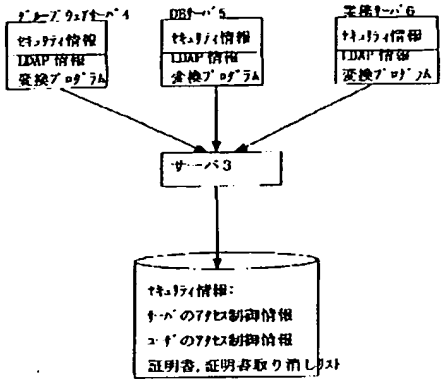
【図1】

図1



【図2】

図2



【図3】

図3

文書XXの定義:
文書識別情報: 文書ID, 業務サーバ6, 組織名称, 文書タイトル, 更新日付, 文書管理者, キーワード, 主題, アブストラクト, 作者名

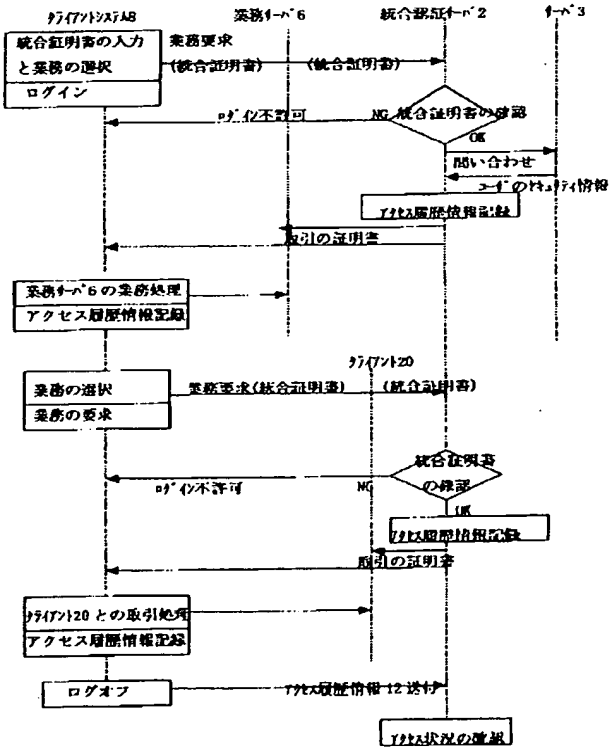
文書XXのアクセス制御情報:
アクセス制御情報, 最終修正情報, セキュリティポリシー

業務サーバ6のドメインセキュリティの定義:
ACL情報: アクセス制御情報20, 管理元は統合認証サーバ2
ドメインセキュリティの定義更新日付, デフォルトセキュリティポリシー, 認可セキュリティポリシー

証明書情報:
ユーザ1の証明書, ・・・・
業務サーバ6の証明書

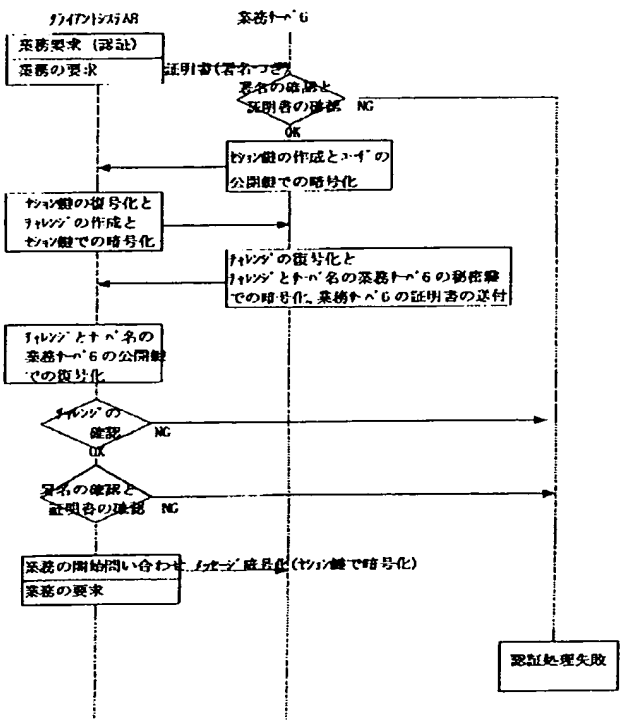
【図5】

図5



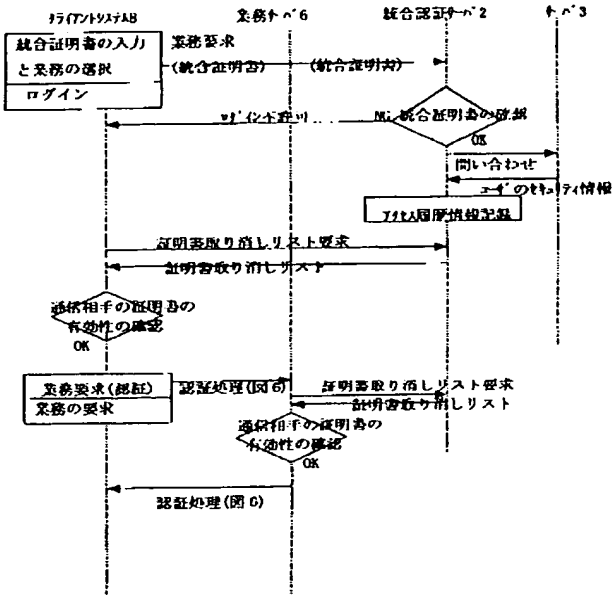
【図6】

図6


クライアントシステムA
業務サーバ6
業務要求（認証）
業務の要求
証明書（署名つき）
署名の確認と証明書の確認
NG
OK
セション鍵の作成とユーザの公開鍵での暗号化
セション鍵の復号化とチャレンジの作成とセション鍵での暗号化
チャレンジの復号化とチャレンジとサーバ名の業務サーバ6の秘密鍵での暗号化、業務サーバ6の証明書の送付
チャレンジとサーバ名の業務サーバ6の公開鍵での復号化
チャレンジの確認
NG
OK
署名の確認と証明書の確認
NG
業務の開始問い合わせ、メッセージ暗号化（セション鍵で暗号化）
業務の要求
認証処理失敗

【図7】

図7


クライアントシステムB
業務サーバ6
統合認証サーバ2
サーバ3
統合証明書の入力と業務の選択
ログイン
業務要求
（統合証明書）
（統合証明書）
NG：統合証明書の確認
OK
問い合わせ
ユーザのセキュリティ情報
アクセス履歴情報記録
証明書取り消しリスト要求
証明書取り消しリスト
通信相手の証明書の有効性の確認
OK
業務要求（認証）
業務の要求
認証処理（図6）
証明書取り消しリスト要求
証明書取り消しリスト
通信相手の証明書の有効性の確認
OK
認証処理（図6）